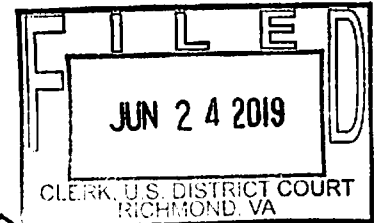


UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

806 Georgiana Court E, Apartment C,
Richmond, Virginia 23236

Case No. 3:19-sw-190

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
806 Georgiana Court E, Apartment C, Richmond, Virginia, is an apartment that has vinyl siding and is tan in color. The door of the apartment is maroon in color, with a letter "C" is affixed to the door.

located in the EASTERN District of VIRGINIA, there is now concealed (identify the person or describe the property to be seized):

See Attachment B of the attached Affidavit, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252A	Possession, Receipt and Distribution of Child Pornography

The application is based on these facts:

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Anthony Dione

Applicant's signature

Anthony Dione TFO

Printed name and title

Sworn to before me and signed in my presence.

Date: 6/24/2019

City and state: Richmond, VA

/s/ Roderick C. Young
 Roderick C. Young
 United States Magistrate Judge

Printed name and title

Winn, D. J. to Toronto, Ontario

Page 2 of 2

[illegible]

3120 Old Orchard Road, Suite 100
Baltimore, MD 21206

[illegible][illegible]

correlation of neural tension and livability correlates with 11 dimensions of

The proposed addition of (a)(1)(B) is being added to the existing (a)(1)(A) and (a)(1)(C) to read:

January 4 to December 14

It is recommended that the following information be provided to the public:

UNITED STATES GOVERNMENT PRINTING OFFICE: 1967

...bought from the ...

To notifiy us of location of damage call

18 U.S.C. § 853A
18 U.S.C. § 853A

about 6200 based at 100meters on 1

versteht sich als „Bewusstsein“ (v.

[illegible]

Abstract

... ..

01/01/2000 10:00 AM

...continued from page 10...

United States Marine Corps
Robert C. Young

44. Isabelle St. Pierre

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF:
806 Georgiana Court E, Apartment C,
Richmond, Virginia 23236

Case No. 3:19SW190

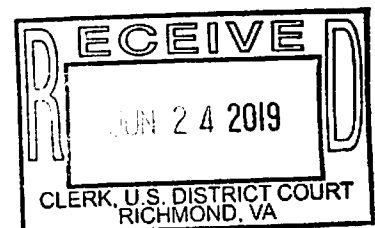
**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Anthony Diocedo, having been first duly sworn, do hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 806 Georgiana Court E, Apartment C, Richmond, Virginia 23236 (hereinafter, the "SUBJECT PREMISES"), further described in Attachment A, for the things described in Attachment B. Attachments A and B are incorporated herein by reference.

2. I, your Affiant, Anthony Diocedo, have been a sworn member of the Chesterfield County Police Department for over 13 years. I have spent approximately four years assigned to various special investigative units. In the course of my employment as a sworn law-enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of Title 18, United States Code §§ 2251, 2252, and 2252A, involving child exploitation and child pornography offenses. I am currently assigned to the Criminal Investigations Division, Special Victims Unit,



as well as a Task Force Officer (“TFO”) assigned to the FBI, Richmond Division, and the Internet Crimes against Children Task Force (“ICAC”) for Southern Virginia. I was deputized as a Special Deputy United States Marshal on October 2, 2018. As a deputized United States Marshal, I am authorized to investigate violations of the laws of the United States and have the authority to execute warrants issued under the authority of the United States.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. I have probable cause to believe that the SUBJECT PREMISES contain contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of: 18 U.S.C. § 2252A (possession, receipt and distribution of child pornography). I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES, as further described in Attachment A and B, incorporated herein by reference, which is located in the Eastern District of Virginia. Located within the SUBJECT PREMISES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer, communication devices, and electronic media located therein where the items specified in Attachment A may be found, and to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of crime.

5. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents, FBI Task Force Agents, and other law-enforcement officers; written reports about this and other investigations that I have received, directly or indirectly, from other law-enforcement agents; information gathered from the service of administrative subpoenas; the

results of physical and electronic surveillance conducted by law-enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training, and background as a detective with the Chesterfield County Police Department. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

DEFINITIONS

6. The following definitions apply to this Affidavit and attachments hereto:

- a. **“Erotica,”** as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.
- b. **“Child Pornography,”** as used herein, is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
- c. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a

visual image, and data which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. See 18 U.S.C. § 2256(5).

- d. **Minor** means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- e. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

TECHNICAL TERMS

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. **“Computer,”** as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”
- b. **“Computer Server” or “Server,”** as used herein is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the

user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

- c. **"Computer hardware,"** as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- d. **"Computer software,"** as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

- e. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. **Digital camera:** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images.

This storage media can contain any digital data, including data unrelated to photographs or videos.

- g. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- h. **GPS:** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected

to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- i. **PDA:** A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- j. **Tablet:** A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, which is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- k. The **“Internet”** is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- l. **“Internet Service Providers” (“ISPs”)**, as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (**“DSL”**) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider (**“ISP”**) over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.
- m. **“Internet Protocol address” or “IP address”** refers to a unique number used by a computer to access the Internet. An IP address is a series of four numbers, each in

the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- n. “The terms **“records,” “documents,”** and **“materials,”** as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), Multi Media Cards (“MMCs”), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- o. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (“HTML”) and is transmitted from web servers to

various web clients via Hyper-Text Transport Protocol ("HTTP").

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

8. On January 14, 2019, your affiant began assisting with an investigation of the dynamic IP address 73.147.76.255, assigned during the time frame discussed below. Special Agent John Houlberg, with the Virginia State Police Bureau of Criminal Investigation, General Investigations Section and assigned to the SOVA ICAC Task Force, initially contacted your affiant regarding the investigation of the dynamic IP address 73.147.76.255. Special Agent Houlberg was previously asked to target IP addresses in Chesterfield County that are actively distributing files of child pornography. Special Agent Houlberg informed your affiant that on December 3, 2018, at 17:38 hours through December 4, 2018, at 05:44 hours he downloaded child pornography from the dynamic IP address 73.147.76.255, while using an automated software program that utilized peer-to-peer (P2P) networks on the Internet. This software program is a free version of the P2P program "Bit Torrent" that has been configured to download files from a single source (single source refers to downloading from a single IP address, as opposed to multiple IP addresses as the default P2P configuration for most P2P applications), record packet traffic, and display geographic locations of IP addresses.

9. Your affiant reviewed the evidence and observed that the automated program successfully achieved a direct connection with IP address 73.147.76.255, on December 3, 2018, at 17:38 GMT -5, through December 4, 2018, at 05:44 GMT -5. The automated program browsed the files that were currently being shared by that IP address during the aforementioned sessions. The automated program detected suspected child pornography files based on known child pornography videos with matching digital algorithms referred to as "SHA1 Values." Based

on this information, the automated program successfully downloaded several of the child pornography files.

10. Your affiant reviewed the downloaded files named "2011 PTHC girl 9yo sucks her brother 5yo boys girls pedo 2011 NEW sex strip fun 9999986.avi", "Katerina – 11 Yo girl From St Petersburg Russia Better To Eat Avi (Pthc – Win Brother Sister – v2- 1.avi", and "(Pthc) Open-f13 – 12Yo Boy & 11Yo Sister Have Petting.avi."

- a. File name: 2011 PTHC girl 9yo sucks her brother 5yo boys girls pedo 2011 NEW sex strip fun 9999986.avi. The video file shows one prepubescent male between the approximate ages of 4 and 6 years old standing nude with his penis exposed while another prepubescent female between the approximate ages of 8 and 10 sits near the camera. The female then places the male's penis in her mouth and fellates him. The female then places the male's penis in her mouth again. The female then exposes her breasts and dances.
- b. File name: Katerina – 11 Yo girl From St Petersburg Russia Better To Eat Avi (Pthc – Win Brother Sister – v2- 1.avi. The video file shows a pubescent female between the approximate age of 11 and 13 years old and a pubescent male between the approximate age of 11 and 13. The female performs fellatio on the male and he performs cunnilingus on her. They then engage in vaginal sex.
- c. File name: (Pthc) Open-f13 – 12Yo Boy & 11Yo Sister Have Petting.avi. The video file shows a fully nude prepubescent female between the approximate age of 10 and 12 years old and a fully nude prepubescent male between the approximate age of 11 and 13 years old. They are initially mutually masturbating

each other. The female then performs fellatio on the male. The female then lays under the male and performs fellatio on him while he rubs her vagina.

11. Your affiant conducted a check of the American Registry for Internet Numbers ("ARIN") and determined that Comcast holds the registration for IP address 73.147.76.255. Based on this information, an administrative subpoena was submitted to Comcast on March 26, 2019, requesting subscriber information for the Comcast user assigned IP address 73.147.76.255 on December 3, 2018, at 17:38:23 GMT -5.

12. Results from the administrative subpoena revealed the following information about IP address 73.147.76.255 during the aforementioned timeframe: (1) the subscriber was "David Sizemore"; (2) the address listed for the account was the SUBJECT PREMISES; (3) the phone number associated with the account was "***-***-9349"; and (4) the listed email address was "davidnsizemore@comcast.net." Comcast records indicated that the dynamic IP address 73.147.76.255, was assigned to the SUBJECT PREMISES beginning on at least September 30, 2018, at 05:03:12, through March 26, 2019, at 00:00:00.

13. A search of publically available records indicates that David Sizemore is associated with the SUBJECT PREMISES in Chesterfield County. One search indicated that David Sizemore began living at the SUBJECT PREMISES in August 2017. A search of the Virginia Employment Commission records indicated that David Sizemore is employed by Southern Police Equipment Incorporated.

14. A search of records of the Virginia Department of Motor Vehicles ("DMV") regarding the name "David Sizemore." Virginia DMV records indicates that David N Sizemore, is associated with the SUBJECT PREMISES, in Chesterfield County. DMV records indicates that

David Sizemore has a vehicle registered in his name: a 2014 Smart Fortwo Coupe bearing Virginia registration ATCVFR.

15. A search of publically available records indicated that a Derek Sizemore is also associated with the SUBJECT PREMISES, in Chesterfield County. One search indicated that Derek Sizemore began living at the SUBJECT PREMISES in March 2015. A search of the Virginia Employment Commission records indicated that Derek Sizemore is employed by Commonwealth of Virginia.

16. Your affiant conducted a search of records of the Virginia DMV regarding the name "Derek Sizemore." Virginia DMV records indicate that Derek A. Sizemore is associated with the SUBJECT PREMISES, in Chesterfield County. DMV records indicate that Derek Sizemore has a vehicle registered in his name: a 2017 Mazda 3 bearing Virginia registration VWB2512.

17. On April 2, 2019, your affiant conducted a spot surveillance of the dwelling located at the SUBJECT PREMISES, in Chesterfield County and photographed the exterior of the residence (see attached image in Attachment A). Your affiant observed that the residence is part of the Aston Ridge apartment complex. The apartments have vinyl siding that is tan in color. The door of the SUBJECT PREMISES is maroon in color, with a letter "C" is affixed to the door. There is a sliding glass door leading out to a patio in the front of the apartment, which is on the first floor. During the surveillance and while standing directly in front of the SUBJECT PREMISES, your affiant used a wireless network detection device and detected approximately 54 wireless networks operating in the immediate vicinity of the SUBJECT PREMISES. Of the 54 wireless networks, 11 were secured with encryption. There were 31 networks that were labeled with the prefix "XFINITY," which your affiant is aware is a Comcast product. Your affiant is also aware

that Comcast requires account holders to log onto all “XFINITY” Wi-Fi networks using their account credentials and passwords, thereby making all Comcast “XFINITY” Wi-Fi networks secure. Further, while standing directly in front of the SUBJECT PREMISES, the secure network with one of the strongest Wi-Fi signals was named “Dnsizemore.”

18. Taken together, the above information indicates that on December 3, 2018, at 1738 GMT -5 through December 4, 2018 at 0544 GMT -5, a person using a computer(s) located at the SUBJECT PREMISES, was using a computer(s) with the dynamic IP address 73.147.76.255 assigned on December 3, 2018, at 1738 GMT -5 through December 4, 2018 at 0544 GMT -5 to download, store, and distribute child pornography files through a file-sharing program on the Bit Torrent Network (i.e. Internet). Based on information provided in this Affidavit, your affiant believes that probable cause exists that child pornography is being stored on a computer(s) in the possession of an individual(s) who resides at the dwelling located at the SUBJECT PREMISES, in Chesterfield County.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT
TO VIEW, COLLECT, RECEIVE CHILD PORNOGRAPHY AND SEEK TO
SEXUALLY EXPLOIT CHILDREN**

19. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who utilize web-based sites to seek children to sexually exploit them by having sexual encounters or obtaining images of child pornography:

- a. Individuals who access with intent to view, possess, collect, receive and distribute child pornography may receive sexual gratification, stimulation, and satisfaction from

contact with children; or from fantasies they may have viewing children engaged in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who access with intent to view, possess, collect and receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who access with intent to view, possess, collect and receive child pornography almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who access with intent to view, possess, collect and receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding

area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals who access with intent to view, possess, collect and receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals involved in sexually exploiting children and who would have knowledge about how to access a hidden and embedded bulletin board would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images and children victims of sexual exploitation. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who access with intent to view, possess, collect and receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Individuals involved in sexually exploiting children sometimes have double lives and concealed forms of communication with these victims. These individuals also create fictitious profiles pertaining to web base accounts such as emails, chatting and forum sites. These individuals with double lives can be involved in children related activities in order to have direct access to new victims. It is common for these individuals to use mobile devices connected to public Wi-Fi internet to communicate with victims and schedule dates for sexual encounters.

i. Individuals who are child predators and sexually exploit children search for children who are vulnerable and easily manipulated. These individuals seek for children with low self-esteem and who are experiencing problems at home.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

20. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. It has also revolutionized the methods that individuals will use to interact with and sexually exploit children. Computers serve four functions in connection with child pornography: production, communication, distribution, and storage.

21. **Production.** Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera

are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

22. Distribution and Communication. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

23. Storage. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which

are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Media storage devices can easily be concealed and carried on an individual’s person.

24. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

25. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer or external media in most cases.

26. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often

are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be

connected and carried on an individual's person.

24. The Internet affords individuals several different venues for obtaining, viewing, and

uploading child pornography in a relatively secure and anonymous fashion.

25. Individuals also use online resources to receive and store child pornography, including

services offered by Internet Forums, such as Yahoo! and Hotmail, among others. The online

services allow a user to set up an account with a remote computing service that provides e-mail

services as well as electronic storage of computer files in any variety of formats. A user can set

up an online storage account from any computer with access to the Internet. Even in cases where

online storage is used, however, evidence of child pornography can be found on the user's

computer or external media in most cases.

26. As is the case with most digital technology, communication by way of computer can be

saved or stored on the computer used for these purposes. Storing this information can be

intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's

favorite websites in, for example, "bookmarked" files. Digital information can also be retained

unintentionally, e.g., traces of the path of an electronic communication may be automatically

stored in many places (e.g., temporary files or ISP client software, among others). In addition to

electronic communications, a computer user's Internet activities generally leave traces or

"footprints" in the web cache and history files of the browser used. Such information is often

maintained indefinitely until overwritten by other data.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

27. As described above and in Attachment B, this application seeks permission to search for records that might be found in the SUBJECT PREMISES in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

28. *Probable cause.* I submit that if a computer or storage medium is found in the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

Depending on a variety of factors, a particular computer could easily not overwrite deleted files with new data for many months, and in certain cases, conceivably ever.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable

cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates)

may be evidence of who used or controlled the computer or storage medium at a relevant time.

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to engage in a child pornography offense (whether it be to produce, distribute, transport, receive or possess child

pornography), the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: 1) data that is evidence of how the computer was used; 2) data that was sent or received; 3) notes as to how the criminal conduct was achieved; 4) records of Internet discussions about the crime; and 5) other records that indicate the nature of the offense.

30. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the SUBJECT PREMISES, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who

has used it requires considerable time, and taking that much time in the SUBJECT PREMISES could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data in the SUBJECT PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media

that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

32. Because multiple people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

SPECIFICITY OF SEARCH WARRANT RETURN

33. Consistent with the Court's current policy, the search warrant return will list the model(s) and serial number(s) of any and all computers seized at the SUBJECT PREMISES and include a general description of any and all associated peripheral equipment that has been seized. Additionally, the search warrant return will include the total numbers of each type of digital media that has been seized (*e.g.*, "ten (10) 3.5" diskettes; twenty (20) CDs; twenty (20) DVDs; three (3) USB drives; one (1) 256 MB flash memory card," etc.)

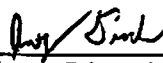
NOTICE REGARDING INITIATION OF FORENSIC EXAMINATION

34. Moreover, the Government will file a written pleading in this case within 120 days after the execution of the search warrant notifying the court that the imaging process of digital evidence seized from the target location is complete, and the forensic analysis of computers and media has begun. Such notice will include confirmation that written notice has been provided to the defendant or his counsel informing the defendant that the forensic examination of evidence seized from him has actually begun. Such notice to the defendant and the Court is not intended to mean, and should not be construed to mean, that the forensic analysis is complete, or that a written report detailing the results of the examination to date will be filed with the Court or provided to the defendant or his counsel. This notice does not create, and is not meant to create, additional discovery rights for the defendant. Rather, the sole purpose of this notice is to notify the defendant that, beyond the simple seizure of his property, a forensic search of that property has actually begun.

CONCLUSION

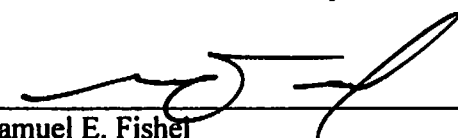
35. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES, authorizing the seizure and search of the items described in Attachment B.

Respectfully submitted,



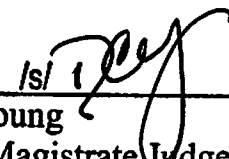
Anthony Diocedo
Task Force Officer
Federal Bureau of Investigation

Seen and approved by:



Samuel E. Fisher
Special Assistant United States Attorney

Sworn to me this 24 day of June 2019



/s/ Roderick C. Young
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF:
806 Georgiana Court E, Apartment C,
Richmond, Virginia 23236

Case No. _____

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The location known as 806 Georgiana Court E, Apartment C, Richmond, Virginia 23236 ("SUBJECT PREMISES") is identified as a residence located in the Aston Ridge apartment complex. The apartments have vinyl siding that is tan in color. The door of the SUBJECT PREMISES is maroon in color, with a letter "C" is affixed to the door. There is a sliding glass door leading out to a patio in the front of the apartment. See below:



IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF:
806 Georgiana Court E, Apartment C,
Richmond, Virginia 23236

Case No. _____

ATTACHMENT B

EVIDENCE TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. § 2252A (possession, receipt, and distribution of child pornography).

1. Computers or storage media used as a means to commit the violations described above.
2. GPS devices
3. Any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence

of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

5. Child pornography and child erotica.

6. Any cameras capable of producing paper or digital photographs and/or audio-visual recordings

7. Records, information, and items relating to violations of the statutes described above including

- a. Records, information, and items relating to the occupancy or ownership of 806 Georgiana Court E, Apartment C, Richmond, Virginia 23236, including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes and ownership of vehicles at the SUBJECT PREMISES;
- b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and
- c. Records and information relating to sexual exploitation of children.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.